

文章编号:1005-3085(2011)01-0055-06

## 由单个状态生成的有限自动机的一些性质\*

黄飞丹<sup>1,2</sup> 蒙春风<sup>1</sup>, 邓培民<sup>1</sup>, 易 忠<sup>1</sup>

(1- 广西师范大学数学科学学院, 桂林 541004; 2- 毕节学院数学系, 贵州 毕节 551700)

**摘 要:** 本文研究了由单个状态生成的有限自动机的弱可逆性及分解, 得出了由单个状态生成的有限自动机弱可逆的充分必要条件, 证明了由单个状态生成的延迟  $\tau$  步弱可逆有限自动机  $M$  能分解为一个延迟 0 步弱可逆有限自动机和一个  $\tau$  阶延迟元的充要条件是  $M$  的生成子的  $\tau$  长输出权为 1.

**关键词:** 线性有限自动机; 可逆; 弱可逆; 弱逆; 分解

**分类号:** AMS(2000) 11B85

**中图分类号:** TP301.1

**文献标识码:** A

### 1 引言

有限自动机是研究离散数字系统的功能、结构及两者关系的数学理论, 它作为一种工具有着广泛的应用. 八十年代, 我国著名学者陶仁骥先生提出了一种基于有限自动机的公钥密码体制和数字签名, 显示了有限自动机在通信领域的重要作用. 这一体制的提出刺激了有限自动机可逆性和有限自动机的化合与分解的研究<sup>[1-7]</sup>. 一般地, 一个有限自动机总可以分解为有限个由单个状态生成的有限自动机的并, 文献[8]主要讨论了由单个状态生成的状态自动机的性质, 文献[9]充分说明了由零状态生成的有限自动机对一般线性有限自动机弱可逆性的研究有很大的作用, 这在一定程度上显示了研究由单个状态生成的有限自动机的意义. 本文研究了由单个状态生成的有限自动机的可逆性及其分解, 得出了由单个状态生成的有限自动机的可逆性与其生成子的关系, 以及由单个状态生成的延迟  $\tau$  步弱可逆有限自动机可分解出  $\tau$  阶延迟元的充要条件. 这对研究一般有限自动机的可逆性和一般延迟  $\tau$  步弱可逆有限自动机的分解是有意义的.

以下未写出的概念和记号可参考文献[9,10].

### 2 可逆性

**定义 1** 称有限自动机  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由单个状态生成的有限自动机, 如果存在  $s_0 \in S$ , 对任何  $s \in S$ , 存在  $\alpha \in X^*$ , 使得  $S = \delta(s_0, \alpha)$ , 即  $S = \{\delta(s_0, \alpha) | \alpha \in X^*\}$ . 这时称  $s_0$  为  $M$  的生成子. 显然, 强连通有限自动机为由单个状态生成的有限自动机.

**定理 1** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  是一个有限自动机,  $s_0 \in S$ , 且  $M$  由  $s_0$  生成, 则  $M$  是弱可逆的当且仅当  $s_0$  是弱可逆的.

**推论 1** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  是一个有限自动机,  $B$  为  $S$  的反向底, 则  $M$  是弱可逆的当且仅当  $B$  中的状态都弱可逆.

收稿日期: 2007-08-07. 作者简介: 黄飞丹 (1981年8月生), 女, 硕士. 研究方向: 环模与自动机理论.

\*基金项目: 国家自然科学基金 (60473005); 广西自然科学基金 (0832103); 广西研究生教育创新计划资助项目 (2007106020701M48).

**定义2**  $M = \langle X, Y, S, \delta, \lambda \rangle$ ,  $M' = \langle Y, X, S', \delta', \lambda' \rangle$  是有限自动机, 对  $s \in S$ , 若存在  $s' \in S'$ , 使得对任何  $\alpha \in X^\omega$ , 有  $\lambda'(s', \lambda(s, \alpha)) = \alpha_0 \alpha$ , 其中  $|\alpha| = \tau$ , 则称  $s'$  为  $s$  的延迟  $\tau$  步弱逆. 对  $s' \in S'$ , 若存在  $s \in S$ , 使得  $s'$  是  $s$  的延迟  $\tau$  步弱逆, 则称  $s'$  是延迟  $\tau$  步弱逆.

**命题1** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$ ,  $M' = \langle Y, X, S', \delta', \lambda' \rangle$  是有限自动机,  $s'_0 \in S'$  是  $s_0 \in S$  的延迟  $\tau$  步弱逆, 则对任意的  $\alpha \in X^*$ ,  $\delta'(s'_0, \lambda(s_0, \alpha))$  为  $\delta(s_0, \alpha)$  的延迟  $\tau$  步弱逆.

**推论2** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  由状态  $s_0$  生成, 则  $M$  延迟  $\tau$  步弱可逆当且仅当存在由单个状态生成的有限自动机为  $M$  的延迟  $\tau$  步弱逆.

由文献[10],  $M = \langle X, Y, S, \delta, \lambda \rangle$  延迟  $\tau$  步弱可逆当且仅当存在一个有限自动机为  $M$  的延迟  $\tau$  步弱逆. 然而对  $s_0 \in S$ , 即使  $s_0$  延迟  $\tau$  步弱可逆, 但不一定存在  $s_0$  的延迟  $\tau$  步弱逆, 除非由  $s_0$  生成的  $M$  的子有限自动机延迟  $\tau$  步弱可逆, 即下面的推论.

**推论3** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为有限自动机,  $s_0 \in S$ , 则  $s_0$  存在延迟  $\tau$  步弱逆当且仅当由  $s_0$  生成的  $M$  的子有限自动机  $M_1$  延迟  $\tau$  步弱可逆.

下面对由单个状态生成的线性有限自动机可逆性进行讨论.

**定理2** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  和  $M' = \langle Y, X, S', \delta', \lambda' \rangle$  都是由零状态生成的线性有限自动机,  $M'$  是  $M$  的延迟  $\tau$  步弱逆, 则  $s' \in S'$  是  $\theta_M$  的延迟  $\tau$  步弱逆当且仅当  $G'(z)s' = 0$ , 其中  $G'(z)$  为  $M'$  的自由响应矩阵,  $\theta_M$  表示  $M$  的零状态.

**证明** 记  $M$  和  $M'$  的传输函数矩阵分别为  $H(z)$  和  $H'(z)$ . 由文献[3], 有  $H'(z)H(z) = z^\tau I$ ,  $I$  为单位矩阵.

**必要性** 因为  $s'$  是  $\theta_M$  的延迟  $\tau$  步弱逆, 故对任意的  $\alpha \in X^\omega$ , 有  $\lambda'(s', \lambda(\theta_M, \alpha)) = \alpha_0 \alpha$ , 其中  $\alpha_0 \in X^\tau$ . 则  $G'(z)s' + H'(z)H(z)X(z) = X_{\alpha_0}(z) + z^\tau X(z)$ , 其中  $X(z)$ ,  $X_{\alpha_0}(z)$  分别为  $\alpha$ ,  $\alpha_0$  的生成函数, 而  $M'$  是  $M$  的延迟  $\tau$  步弱逆, 因为  $H'(z)H(z) = z^\tau I$ , 从而  $G'(z)s' = X_{\alpha_0}(z)$ . 另一方面,  $M'$  由零状态  $\theta_{M'}$  生成, 可设  $s' = \delta'(\theta_{M'}, \beta)$ ,  $\beta \in X^k$ ,  $k \geq 0$ , 则

$$\begin{aligned}\lambda'(\theta_{M'}, \beta)\lambda'(s', \lambda(\theta_M, \alpha)) &= \lambda'(\theta_{M'}, \beta)\lambda'(\delta'(\theta_{M'}, \beta), \lambda(\theta_M, \alpha)) \\ &= \lambda'(\theta_{M'}, \beta\lambda(\theta_M, \alpha)) = \lambda'(\theta_{M'}, \beta)\alpha_0\alpha,\end{aligned}$$

即

$$\begin{aligned}&G'(z)\theta_{M'} + H'(z)(X_\beta(z) + z^k H(z)X(z)) \\ &= G'(z)\theta_{M'} + H'(z)X_\beta(z) + z^k(X_{\alpha_0}(z) + z^\tau X(z)),\end{aligned}$$

整理得

$$H'(z)X_\beta(z) + z^k H'(z)H(z)X(z) = H'(z)X_\beta(z) + z^k X_{\alpha_0}(z) + z^{k+\tau} X(z),$$

其中  $X_\beta(z)$  是  $\beta$  的生成函数, 从而  $z^k X_{\alpha_0}(z) = 0$ , 所以  $G'(z)s' = X_{\alpha_0}(z) = 0$ .

**充分性** 设  $s' \in S'$  满足  $G'(z)s' = 0$ , 则对任意的  $\alpha \in X^\omega$ ,  $\lambda'(s', \lambda(\theta_M, \alpha))$  的生成函数为

$$G'(z)s' + H'(z)(G(z)\theta_M + H(z)X(z)) = G'(z)s' + H'(z)H(z)X(z) = z^\tau X(z),$$

所以  $\lambda'(s', \lambda(\theta_M, \alpha)) = \alpha_0 \alpha$ , 其中  $\alpha_0$  为  $\tau$  长零序列. 所以  $s'$  是  $\theta_M$  的延迟  $\tau$  步弱逆.

由此可知, 这时  $M'$  的零状态  $\theta_{M'}$  是  $\theta_M$  的延迟  $\tau$  步弱逆, 但  $\theta_M$  的延迟  $\tau$  步弱逆可能不只是  $\theta_{M'}$ .

**命题 2** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  是由零状态生成的线性有限自动机, 则  $M' = \langle Y, X, S', \delta', \lambda' \rangle$  是  $M$  的延迟  $\tau$  步弱逆当且仅当存在  $s' \in S'$ , 使得对任意的  $\alpha \in X^\omega$ ,  $\lambda'(s', \lambda(\theta_M, \alpha)) = \alpha_0 \alpha$ , 其中  $\theta_M$  是  $M$  的零状态,  $|\alpha_0| = \tau$ .

**证明** 只证充分性. 对任意的  $s \in S$ ,  $\alpha \in X^\omega$ , 因为  $M$  由零状态生成, 所以必存在  $\beta \in X^*$ , 使得  $s = \delta(\theta_M, \beta)$ , 则  $\lambda(s, \alpha) = \lambda(\delta(\theta_M, \beta), \alpha)$ , 而

$$\lambda(\theta_M, \beta) \lambda(s, \alpha) = \lambda(\theta_M, \beta) \lambda(\delta(\theta_M, \beta), \alpha) = \lambda(\theta_M, \beta \alpha),$$

由条件存在  $s' \in S'$ , 使得  $\lambda'(s', \lambda(\theta_M, \beta \alpha)) = \alpha_0 \beta \alpha$ ,  $|\alpha_0| = \tau$ , 即

$$\begin{aligned} \lambda'(s', \lambda(\theta_M, \beta \alpha)) &= \lambda'(s', \lambda(\theta_M, \beta) \lambda(s, \alpha)) \\ &= \lambda'(s', \lambda(\theta_M, \beta)) \lambda'(\delta'(s', \lambda(\theta_M, \beta)), \lambda(s, \alpha)) = \alpha_0 \beta \alpha = \alpha' \alpha'_0 \alpha, \end{aligned}$$

其中  $|\alpha'| = |\beta|$ , 那么  $|\alpha'_0| = \tau$ , 从而存在状态  $\delta'(s', \lambda(\theta_M, \beta))$ , 使得

$$\lambda'(\delta'(s', \lambda(\theta_M, \beta)), \lambda(s, \alpha)) = \alpha'_0 \alpha, \quad |\alpha'_0| = \tau,$$

由  $s$  的任意性知  $M'$  是  $M$  的延迟  $\tau$  步弱逆.

**命题 3**  $M = \langle X, Y, S, \delta, \lambda \rangle$  是由零状态生成的线性有限自动机,  $M' = \langle Y, X, S', \delta', \lambda' \rangle$  是线性有限自动机, 且满足对任意的  $s' \in S'$ ,  $\beta \in X^*$ , 存在  $s'_0 \in S'$ , 使得

$$s' = \delta'(s'_0, \lambda(\theta_M, \beta)),$$

则  $M'$  是  $M$  的延迟  $\tau$  步逆当且仅当对任意的  $s' \in S'$ ,  $\alpha \in X^\omega$ , 存在  $\alpha_0 \in X^\tau$ , 使得

$$\lambda'(s', \lambda(\theta_M, \alpha)) = \alpha_0 \alpha.$$

### 3 分解

设  $M_1 = \langle X, Y, S_1, \delta_1, \lambda_1 \rangle$ ,  $M_2 = \langle Y, Z, S_2, \delta_2, \lambda_2 \rangle$  是有限自动机,  $M_1$  与  $M_2$  的合成(或化合)定义为  $C(M_1, M_2) = \langle X, Z, S_1 \times S_2, \delta, \lambda \rangle$ , 其中

$$\delta(\langle s_1, s_2 \rangle, x) = \langle \delta_1(s_1, x), \delta_2(s_2, \lambda_1(s_1, x)) \rangle,$$

$$\lambda(\langle s_1, s_2 \rangle, x) = \lambda_2(s_2, \lambda_1(s_1, x)), \quad \langle s_1, s_2 \rangle \in S_1 \times S_2, \quad x \in X.$$

也记为  $M_1 \circ M_2$ .

弱可逆有限自动机  $M$  简记为 WIFA  $M$ . 称 WIFA  $M$  是可分解的, 如果存在两个 WIFA  $M_1$  和  $M_2$ , 使得  $M \prec M_1 \circ M_2$ .

**定义 3<sup>[1]</sup>** 称有限自动机  $M = \langle X, X, X, \delta, \lambda \rangle$  为一个延迟元, 其中

$$\delta(x, x') = x', \quad \lambda(x, x') = x, \quad \forall x, x' \in X,$$

记为  $M_d$ .  $\tau$  个  $M_d$  的合成记为  $M_{\tau d}$ , 并称之为  $\tau$  阶延迟元.

沿用文献 [1,2] 的记号, 对有限自动机  $M = \langle X, Y, S, \delta, \lambda \rangle$ , 对  $M$  的任一状态  $s$  及正整数  $r$ , 以下令

$$W_{r,s}^M = \{ \lambda(s, x_0, \dots, x_{r-1}) \mid x_0, \dots, x_{r-1} \in X \},$$

称为  $s$  的长  $r$  输出集. 称

$$|W_{r,s}^M| \text{ 和 } \omega_{r,M} = \min_{s \in S} |W_{r,s}^M|$$

为  $s$  的长  $r$  输出权及  $M$  的长  $r$  极小输出权.

设  $M = \langle X, Y, S, \delta, \lambda \rangle$  是一个有限自动机,  $s \in S, y \in Y$ , 定义

$$Out(s) = \{\lambda(s, x) \mid x \in X\}, \quad d(s) = |Out(s)|,$$

$$S_t(s, y) = \{t \in S \mid \exists x \in X, \text{ s.t. } t = \delta(s, x) \text{ and } \lambda(s, x) = y\}.$$

**命题4** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由  $s_0 \in S$  生成的严格延迟1步 WIFA,  $|X| = |Y|$ , 且对任意  $s \in S, d(s_0) \leq d(s)$ , 则  $M$  的所有状态的延迟步数都为1.

**证明** 设  $|X| = |Y| = n$ , 因为  $M$  是严格延迟1步弱可逆的, 所以对任意的  $s \in S, delay(s) \leq 1$  ( $delay(s)$  表示  $s$  的延迟步数 [2]). 由于  $d(s_0)$  最小, 故  $d(s_0) < n$ . 否则由文献 [4] 的定理2, 对任意的  $s' \in S, d(s') = d(s_0) = n$ , 由于  $|X| = |Y| = n$ , 故对任意的  $s' \in S$ , 若  $\lambda(s', x) = \lambda(s, y), x, y \in X$ , 则  $x = y$ , 从而  $s'$  延迟0步弱可逆. 这与  $M$  严格延迟1步弱可逆矛盾. 从而  $d(s) = d(s_0) < n, s$  不延迟0步弱可逆, 故  $s$  延迟1步弱可逆,  $delay(s) = 1$ .

**命题5** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由  $s_0 \in S$  生成的严格延迟1步 WIFA,  $|X| = |Y|$  为素数, 且对任意  $s \in S, d(s_0) \leq d(s)$ , 则对任意  $s \in S, d(s) = 1$ . 设  $x_1, \dots, x_n$  是  $X$  上的一个排列, 则对任意  $s \in S, Out(\delta(s, x_1)), \dots, Out(\delta(s, x_n))$  是  $Y$  上的一个排列.

**定理3** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由  $s_0 \in S$  生成的严格延迟1步 WIFA,  $|X|$  为素数, 且对任意  $s \in S, d(s_0) \leq d(s)$ , 则存在延迟0步 WIFA  $M_0$ , 使得  $M \prec M_0 \circ M_d$ .

**证明** 由命题5, 对任意的  $s \in S, d(s) = 1$ , 即对任意的  $x, x \in X$ , 有  $\lambda(s, x) = \lambda(s, x')$ . 如文献 [1] 构造有限自动机  $M_0 = \langle X, X, S, \delta_0, \lambda_0 \rangle$ , 其中

$$\delta_0(s, x) = \delta(s, x), \quad \lambda_0(s, x) = \lambda(\delta(s, x)), \quad \forall s \in S, x \in X.$$

$M_0$  是一个延迟0步弱可逆有限自动机. 容易证明  $M \prec M_0 \circ M_d$ .

**命题6** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由  $s_0 \in S$  生成的延迟  $\tau$  步 WIFA,  $|X| = |Y| = n$ , 则  $|W_{r,s_0}^M| = \omega_{r,M}$  当且仅当对任何  $s, s' \in S, |W_{r,s}^M| = |W_{r,s'}^M|$ .

**证明** 只证必要性. 对任意的  $s \in S$ , 设  $s = \delta(s_0, \alpha)$ , 由于  $|W_{r,s_0}^M| = \omega_{r,M}$ , 由文献 [11] 命题2, 有  $|W_{r,s}^M| = \omega_{r,M}$ , 故对任意的  $s, s' \in S, |W_{r,s}^M| = |W_{r,s'}^M|$ .

由文献 [2] 定理3及命题6可得.

**定理4** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由  $s_0 \in S$  生成的延迟  $\tau$  步 WIFA,  $|X| = |Y| = n > 1$ , 则  $M$  可分解为一个延迟0步 WIFA 和一个  $\tau$  阶延迟元当且仅当  $|W_{r,s_0}^M| = 1$ .

**推论4** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由零状态生成的延迟  $\tau$  步弱可逆线性有限自动机, 且对任意  $s \in S^\tau = \{\delta(\theta_M, \alpha) \mid \alpha \in X^k, k \geq \tau\}, \lambda(s, 0) = 0$ , 则  $M$  不能分解为一个延迟0步 WIFA 和一个  $\tau$  阶延迟元.

**证明** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  是由零状态生成的延迟  $\tau$  步弱可逆线性有限自动机, 若  $M$  能分解为一个延迟0步 WIFA 和一个  $\tau$  阶延迟元, 由定理4, 有  $|W_{r,\theta_M}^M| = 1$ . 即对任意  $\alpha_1, \alpha_2 \in X^\tau, \alpha_1 \neq \alpha_2, \lambda(\theta_M, \alpha_1) = \lambda(\theta_M, \alpha_2)$ , 由条件知  $\lambda(\theta_M, \alpha_1 0^\omega) = \lambda(\theta_M, \alpha_2 0^\omega)$ . 记  $\alpha_1 0^\omega, \alpha_2 0^\omega$  的生成函数分别为  $X_1(z), X_2(z)$ ,  $M$  的传输函数矩阵为  $H(z)$ , 则  $H(z)X_1(z) = H(z)X_2(z)$ , 即  $H(z)[X_1(z) - X_2(z)] = 0$ , 由文献 [11] 的定理1知  $X_1(z) - X_2(z) = 0$ , 即  $X_1(z) = X_2(z)$ , 故  $\alpha_1 0^\omega = \alpha_2 0^\omega$ , 即  $\alpha_1 = \alpha_2$ . 这与  $\alpha_1 \neq \alpha_2$  矛盾. 所以命题成立.

**推论 5** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$  为由  $s_0 \in S$  生成的严格延迟 1 步 WIFA,  $|X| = |Y| = n > 1$ ,  $|W_{1,s_0}^M| = \omega_{1,M}$ , 则  $M$  不可分解为一个延迟 0 步 WIFA 和一个 1 阶延迟元当且仅当  $n$  为合数且  $\omega_{1,M} \neq 1$ .

**例 1** 设  $M = \langle X, Y, S, \delta, \lambda \rangle$ , 其中  $X = Y = \{a, b, c, d, e, f\}$ ,  $S = \{s_1, s_2\}$ ,  $\delta$  和  $\lambda$  定义如下:

$$\begin{aligned} \delta(s_1, a) &= s_1, & \lambda(s_1, a) &= a; & \delta(s_2, a) &= s_1, & \lambda(s_2, a) &= d; \\ \delta(s_1, b) &= s_2, & \lambda(s_1, b) &= a; & \delta(s_2, b) &= s_2, & \lambda(s_2, b) &= d; \\ \delta(s_1, c) &= s_1, & \lambda(s_1, c) &= b; & \delta(s_2, c) &= s_1, & \lambda(s_2, c) &= e; \\ \delta(s_1, d) &= s_2, & \lambda(s_1, d) &= b; & \delta(s_2, d) &= s_2, & \lambda(s_2, d) &= e; \\ \delta(s_1, e) &= s_1, & \lambda(s_1, e) &= c; & \delta(s_2, e) &= s_1, & \lambda(s_2, e) &= f; \\ \delta(s_1, f) &= s_2, & \lambda(s_1, f) &= c; & \delta(s_2, f) &= s_2, & \lambda(s_2, f) &= f. \end{aligned}$$

易知,  $M$  为由单个状态生成的有限自动机,  $s_1, s_2$  都是  $M$  的生成子. 易证  $M$  分解不出延迟元. 这再一次否定了文献 [1] 提出的公开问题: 严格延迟  $\tau$  步弱可逆且每个状态的延迟步数均为  $\tau$  的  $n$  元 WIFA  $M$  是否一定可分解出延迟元?

## 参考文献:

- [1] 鲍丰. 弱可逆有限自动机的化合与分解[J]. 中国科学: A 辑, 1993, 23(7): 759-765  
Bao F. Composition and decomposition of weakly invertible finite automata[J]. Science in China, Series A, 1993, 23(7): 759-765
- [2] 王鸿吉. 分解弱可逆有限自动机的两个结果[J]. 计算机研究与发展, 2005, 42(4): 690-696  
Wang H J. Two results of decomposing weakly invertible finite automata[J]. Journal of Computer Research and Development, 2005, 42(4): 690-696
- [3] 曹锋, 邓培民, 易忠. 弱可逆有限自动机的分解[J]. 计算机学报, 2005, 28(9): 1501-1507  
Cao F, Deng P M, Yi Z. Decomposition of weakly invertible finite automata[J]. Chinese Journal of Computers, 2005, 28(9): 1501-1507
- [4] 阎航宇, 谢正卫, 邓培民等. 线性有限自动机零状态的作用[J]. 广西师范大学学报: 自然科学版, 2006, 24(1): 30-33  
Yan H Y, Xie Z W, Deng P M, et al. Functions of zero state of linear finite automata[J]. Journal of Guangxi Normal University (Natural Science Edition), 2006, 24(1): 30-33
- [5] 高翔, 鲍丰. 二元弱可逆有限自动机延迟步数的分解[J]. 计算机学报, 1994, 17(5): 330-337  
Gao X, Bao F. Decomposition of binary weakly invertible finite automata[J]. Chinese Journal of Computers, 1994, 17(5): 330-337
- [6] 高翔. 关于弱可逆有限自动机延迟步数分解的两个结果[J]. 计算机学报, 1993, 16(8): 629-632  
Gao X. Two results about the decomposition of delay step of weakly invertible finite automata[J]. Chinese Journal of Computers, 1993, 16(8): 629-632
- [7] 曹锋, 邓培民, 易忠. 关于 Moore 自动机可逆性的一些结果[J]. 广西师范大学学报: 自然科学版, 2003, 21(4): 44-47  
Cao F, Deng P M, Yi Z. Some results of invertibility of moore automata[J]. Journal of Guangxi Normal University (Natural Science Edition), 2003, 21(4): 44-47
- [8] 沈虹. 自动机的半群结构[J]. 数学学报, 1987, 30(5): 679-687  
Shen H. Semigroup structure of automata[J]. Acta Mathematica Sinica, 1987, 30(5): 679-687
- [9] 陶仁骥. 有限自动机的可逆性[M]. 北京: 科学出版社, 1979  
Tao R J. Invertibility of Finite Automata[M]. Beijing: Science Press, 1979
- [10] 陶仁骥. 自动机引论[M]. 北京: 科学出版社, 1986  
Tao R J. Introduction to Finite Automata[M]. Beijing: Science Press, 1986

- [11] 戴宗铎, 叶顶锋. 线性有限自动机的可逆性-传输函数的分类与枚举[J]. 中国科学(A辑), 1996, 26(5): 429-436  
Dai Z D, Ye D F. Invertibility of linear finite automata-classification and enumeration of transfer function[J]. Science in China, Series A, 1996, 26(5): 429-436

## Some Characteristics of Finite Automata Generated by Single State

HUANG Fei-dan<sup>1,2</sup>, MENG Chun-feng<sup>1</sup>, DENG Pei-min<sup>1</sup>, YI Zhong<sup>1</sup>

(1- College of Mathematical Science, Guangxi Normal University, Guilin 541004;

2- Department of Mathematics, Bijie College, Bijie, Guizhou 551700)

**Abstract:** This paper investigates the weakly invertible and decomposable properties of the finite automata generated by a single state. To prove whether a finite automation generated by a single state is weakly invertible, some necessary and sufficient conditions are shown. Moreover, for a weakly invertible finite automation (WIFA for short)  $M$  with delay  $\tau$  generated by a single state,  $M$  can be decomposed into a WIFA with delay 0 and a  $\tau$ -order unit if and only if the  $\tau$ -output weight of the generator of  $M$  is 1.

**Keywords:** linear finite automata; invertibility; weak invertibility; weakly inverse; decomposition

---

Received: 07 Aug 2007. Accepted: 18 Sep 2008.

**Foundation item:** The National Natural Science Foundation of China (60473005); the Guangxi Science Foundation (0832103); the Innovation Project of Guangxi Graduate Education (2007106020701M48).